AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Previously Presented) A computer readable medium storing computer executable instructions for connecting to a database, the computer executable instructions comprising functionality to perform the operations of:

receiving, at a launcher application, a request from a user to obtain a file from the database, wherein the database is accessed by a software application, wherein the user logs in to the software application using a user name and a user password, wherein the software application signs on to the database using the user name and a database password, and wherein the database password comprises a hash of the user name and the user password;

obtaining, at the launcher application and in response to the request, a file dump associated with the database and comprising an encrypted database password, wherein the encrypted database password is the database password encrypted using a public encryption key provided by a vendor of the software application, and wherein the encrypted database password is generated by the software application before receiving the request;

decrypting, by the launcher application, the encrypted database password using a private key stored in the launcher application to obtain the database password, wherein the private key is provided by the vendor and stored in the launcher application before receiving the request;

signing on to the database, using the launcher application, with the user name and the database password to obtain a temporary user name, wherein the user name has access to a set of data and functions in the database, wherein the temporary user name is restricted to a subset of the set of data and functions, and wherein the subset has less data and fewer functions than the set;

signing on to the database, using the launcher application, with the temporary user name and the database password;

sending a connect string including the database password and the temporary user name to a database tool; and

accessing the database, using the database tool, to obtain the file stored in the database, wherein the database tool is separate from the launcher application, and wherein the launcher application and the software application execute on different computers.

2. — 12. (Cancelled)

13. (Previously Presented) A system to connect to a database, comprising:

a processor;

an attempted signon module executing on the processor and configured to initiate a signon attempt to the database using a defective signon, wherein the database sends a file dump in response to the signon attempt;

a read module executing on the processor and configured to read an encrypted version of a database password in the file dump, wherein the database password comprises a hash of a user name and a password associated with a user, wherein the user name and the password are used to log in to a software application, and wherein the software application signs on to the database using the user name and the database password;

a decryption module executing on the processor and configured to decrypt the encrypted version of the database password using a private key provided by a vendor of the software application to obtain the database password, wherein the database password is encrypted using a public key provided by the vendor before the signon attempt;

a temporary signon module executing on the processor and configured to signon to the database using the user name and the database password to obtain a temporary user name, and then signon to the database using the temporary user name and the database password, wherein the user name has access to a set of data and functions in the database, wherein the temporary user name is restricted to a subset of the set of data and functions, wherein the subset has less data and fewer functions than the set; and

a pass connect string module executing on the processor and configured to pass a connect string comprising the database password to a database tool,

wherein the database tool, upon receipt of the connect string, requests a file stored in the database and receives the file, and

wherein the temporary signon module and the software application execute on different computers.

14. (Cancelled)

15. (Cancelled)

16. (Cancelled)

17. (Cancelled)

18. (Cancelled)

19. (Previously Presented) A method of controlling a processor to connect to a database, the method comprising:

receiving, at a launcher application, a request from a user to obtain a file stored in the database, wherein the database is accessed by a software application, wherein the user logs in to the software application using a user name and a user password, wherein the software application signs on to the database using the user name and a database password, and wherein the database password comprises a hash of the user name and the user password;

obtaining, at the launcher application and in response to the request, a file dump associated with the database and comprising an encrypted database password, wherein the encrypted database password is the database password encrypted using a public encryption key provided by a vendor of the software application, and wherein the encrypted database password is generated by the software application before receiving the request;

decrypting, by the launcher application, the encrypted database password using a private key stored in the launcher application to obtain the database password, wherein the private key is provided by the vendor and stored in the launcher application before receiving the request;

signing on to the database, using the launcher application, with the user name and the database password to create a temporary user name, wherein the user name has access to a set of data and functions in the database, wherein the temporary user name is restricted to a subset of the set of data and functions, and wherein the subset has less data and fewer functions than the set;

signing on to the database, using the launcher application, with the temporary user name and the database password;

sending a connect string including the database password and the temporary user name and the database password to a database tool; and

accessing the database, using the database tool, to obtain the file stored in the database, wherein the database tool is separate from the launcher application, and wherein the launcher application and the software application execute on different computers.

20. — 30. (Cancelled)

31. (Previously Presented) A computer readable medium storing computer executable instructions for connecting to a database, the computer executable instructions comprising functionality to perform the operations of:

obtaining a user name and a password of a user for logging in to a software application;

creating a database password by hashing the user name and the password, wherein the software application signs on to the database using the user name and the password;

encrypting the database password using a public encryption key provided by a vendor of the software application to create an encrypted database password;

storing the encrypted database password in the database;

receiving, from a launcher application, a signon attempt for the database, wherein the signon attempt fails;

creating a file dump comprising the encrypted password in response to the failed signon attempt;

sending the file dump to the launcher application, wherein the launcher application obtains the database password by decrypting the encrypted database password using a private key provided by the vendor and stored within the launcher application;

generating a temporary user name based on the user name, wherein the user name has access to a set of data and functions in the database, wherein the temporary user name is restricted to a subset of the set of data and functions, and wherein the subset has less data and fewer functions than the set;

granting a request from the launcher application to signon to the database using the temporary user name and the database password;

receiving a request from a database tool for a file stored in the database, wherein the launcher application sends the temporary user name and the database password to the database tool; and

sending the file stored in the database to the database tool, wherein the launcher application and the software application execute on different computers.

32. (Cancelled)

33. (Cancelled)

34. (Currently Amended) A system to connect to a database, comprising:

a processor;

a hash module executing on the processor and configured to hash a user name and a password to create a database password, wherein the user name and the password are used to log in to a software application, and wherein the user name and the database password are used to signon to the database;

an encryption module executing on the processor and configured to create an encrypted version of the database password using a public key provided by a vendor of the software application;

a store module executing on the processor and configured to store the encrypted database password in the database; and

a send module configured to [[to]] send the encrypted database password file to a launcher application in a file dump, wherein the launcher application decrypts the encrypted version of the database password using a private key provided by the software vendor and stored in the launcher application,

wherein the database generates a temporary user name for the launcher application, wherein the temporary user name has access to less data and fewer functions in the database than the user name,

wherein the database grants a request from the launcher application to signon to the database using the temporary user name and the database password, and

wherein the database sends the file stored in the database to a database tool associated with the launcher application in response to a query for the file from the database tool.

35. (Cancelled)

36. (Cancelled)

37. (Previously Presented) A method of controlling a processor to connect to a database and a launcher application, the method comprising:

obtaining a user name and a password of a user for logging in to a software application;

creating a database password by hashing the user name and the password, wherein the software application signs on to the database using the user name and the password;

encrypting the database password using a public encryption key provided by a vendor of the software application to create an encrypted database password;

storing the encrypted database password in the database;

receiving, from a launcher application, a signon attempt for the database after storing the encrypted database password in the database, wherein the signon attempt fails;

creating a file dump comprising the encrypted password in response to the failed signon attempt;

sending the file dump to the launcher application, wherein the launcher application obtains the database password by decrypting the encrypted database password using a private key provided by the vendor and stored within the launcher application;

generating a temporary user name based on the user name, wherein the user name has access to a set of data and functions in the database, wherein the temporary user name is restricted to a subset of the set of data and functions, and wherein the subset has less data and fewer functions than the set;

granting a request from the launcher application to signon to the database using the temporary user name and the database password;

receiving a request from a database tool for a file stored in the database, wherein the launcher application sends the temporary user name and the database password to the database tool; and

sending the file stored in the database to the database tool, wherein the launcher application and the software application execute on difference computers.

38. — 41. (Cancelled)

42. (Previously Presented) The computer readable medium of claim 1, the computer executable instructions comprising functionality to perform the operations of:

initiating, using the launcher application after receiving the request from the user, a signon attempt to the database with a defective signon,

wherein the database generates the file dump in response to the signon attempt.

43. (Previously Presented) The method of claim 19, further comprising:

initiating, using the launcher application after receiving the request from the user, a signon attempt to the database with a defective signon,

wherein the database generates the file dump in response to the signon attempt.